

STEVEN G. KALAR
Federal Public Defender
HANNI M. FAKHOURY
Assistant Federal Public Defender
1301 Clay Street, Suite 1350N
Oakland, CA 94612
(510) 637-3500
hanni_fakhoury@fd.org

Attorneys for DUMAKA HAMMOND

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

UNITED STATES OF AMERICA,)	CR 16-102-JD
)	
Plaintiff,)	MOTION TO SUPPRESS NIT SEARCH
v.)	WARRANT FOR VIOLATING THE
)	FOURTH AMENDMENT
DUMAKA HAMMOND,)	
)	Date: September 8, 2016
Defendant.)	Time: 10:30 a.m.
)	
)	

**TO: BRIAN STRETCH, UNITED STATES ATTORNEY; AND
THOMAS R. GREEN, ASSISTANT UNITED STATES ATTORNEY:**

PLEASE TAKE NOTICE that the defendant DUAMAKA HAMMOND hereby moves this Court for an order suppressing the Network Investigative Technique (“NIT”) search warrant for violating the Fourth Amendment to the United States Constitution. This motion will be heard on September 8, 2016 at 10:30 a.m. in Courtroom 11, on the 19th Floor of the San Francisco Courthouse.

This motion is based on this notice and motion, the attached memorandum of points and authorities and accompanying exhibits, including previously filed exhibits, the Fourth Amendment to the United States Constitution, all other applicable constitutional, statutory and case authority and such evidence and argument that may be presented at the motion hearing.

TABLE OF CONTENTS

INTRODUCTION	1
STATEMENT OF FACTS	1
ARGUMENT	6
A. Each Deployment of the NIT Resulted in a Series of Invasive Searches and Seizures.	6
1. The Presence of the NIT on Mr. Hammond’s Computer Was a Seizure and Search.	7
2. Operating the NIT on Mr. Hammond’s Computer Was a Search.	7
3. Copying Data From Mr. Hammond’s Computer Was a Seizure.....	9
B. The NIT Warrant Was an Unconstitutional General Warrant.	9
1. The Government Chose Not to Provide Additional Information in the Warrant.	10
2. The Warrant Failed to Particularly Describe What Was Being Searched and Where Those Searches Would Occur.	11
3. The Warrant Vested Too Much Discretion in the Executing Officers.	13
CONCLUSION	15

TABLE OF AUTHORITIES**Cases**

<i>Arizona v. Evans</i> , 514 U.S. 1 (1995)	1
<i>Ashcroft v. Free Speech Coalition</i> , 535 U.S. 234 (2002)	12
<i>Boyd v. United States</i> , 116 U.S. 616 (1886)	8
<i>Coolidge v. New Hampshire</i> , 403 U.S. 443 (1971)	9, 14
<i>Go-Bart Importing Co. v. United States</i> , 282 U.S. 344 (1931)	10
<i>Greenstreet v. Cnty. of San Bernardino</i> , 41 F.3d 1306 (9th Cir. 1994)	12
<i>Groh v. Ramirez</i> , 540 U.S. 551 (2004)	11, 14
<i>In re Warrant to Search A Certain Email Account</i> , 2016 WL 377056 (2d Cir. Jul. 14, 2016)	13
<i>In re Terrorist Bombings of U.S. Embassies in East Africa</i> , 552 F.3d 157 (2d Cir. 2008)	13
<i>Katz v. United States</i> , 389 U.S. 347 (1967)	6, 7, 14
<i>LeClair v. Hart</i> , 800 F.2d 692 (7th Cir. 1986)	9
<i>Marron v. United States</i> , 275 U.S. 192 (1927)	13
<i>Maryland v. Garrison</i> , 480 U.S. 79 (1987)	10
<i>Maryland v. King</i> , 133 S. Ct. 1958 (2013)	11
<i>Rakas v. Illinois</i> , 439 U.S. 128 (1978)	8
<i>Riley v. California</i> , 134 S. Ct. 2473 (2014)	7, 8
<i>Stanford v. Texas</i> , 379 U.S. 476 (1965)	13
<i>Steagald v. United States</i> , 451 U.S. 204 (1981)	11
<i>United States v. Bridges</i> , 344 F.3d 1010 (9th Cir. 2003)	13, 14
<i>United States v. Bright</i> , 630 F.2d 804 (5th Cir. 1980)	10
<i>United States v. Cardwell</i> , 680 F.2d 75 (9th Cir. 1982)	10
<i>United States v. Comprehensive Drug Testing, Inc.</i> , 621 F.3d 1162 (9th Cir. 2010)	9, 14
<i>United States v. Cotterman</i> , 709 F.3d 952 (9th Cir. 2013) (en banc)	1, 8
<i>United States v. Crawford</i> , 372 F.3d 1048 (9th Cir. 2004) (en banc)	14
<i>United States v. Duran-Orozco</i> , 192 F.3d 1277 (9th Cir. 1999)	15

1	<i>United States v. Ganoe</i> , 538 F.3d 1117 (9th Cir. 2008)	8
2	<i>United States v. Gourde</i> , 440 F.3d 1065 (9th Cir. 2006).....	12
3	<i>United States v. Hill</i> , 459 F.3d 966 (9th Cir. 2006).....	11
4	<i>United States v. Jacobsen</i> , 466 U.S. 109 (1984)	6, 7, 9
5	<i>United States v. Jefferson</i> , 571 F. Supp. 2d 696 (E.D. Va. 2008)	9
6	<i>United States v. Jones</i> , 132 S. Ct. 945 (2012)	6, 7
7	<i>United States v. Payton</i> , 573 F.3d 859 (9th Cir. 2009)	8
8	<i>United States v. Spilotro</i> , 800 F.2d 959 (9th Cir. 1986).....	11
9	<i>Walter v. United States</i> , 447 U.S. 649 (1980)	12
10	<i>Wong Sun v. United States</i> , 371 U.S. 471 (1963).....	14

Constitutional Provisions

12	U.S. CONST. AMEND. IV	<i>passim</i>
----	-----------------------------	---------------

Federal Statutes

14	18 U.S.C. § 2252(a)(4)(B).....	5
----	--------------------------------	---

Federal Rules

16	Fed. R. Crim. P. 41(b)	13
----	------------------------------	----

News Articles

18	Andy Greenberg, “Over 80 Percent of Dark-Web Visits Relate to Pedophilia, Study Finds,” <i>Wired</i>	
19	(Dec. 30, 2014), <i>available at</i> https://www.wired.com/2014/12/80-percent-dark-web-visits-	
20	relate-pedophilia-study-finds/	12
21	Joseph Cox, “FBI’s Mass Hack Hit 50 Computers in Austria,” <i>Motherboard</i> (Jul. 28, 2016),	
22	<i>available at</i> https://motherboard.vice.com/read/fbis-mass-hack-playpen-operation-pacifier-	
23	hit-50-computers-in-austria	13
24	Joseph Cox, “New Case Suggests the FBI Shared Data from Its Mass Hacking Campaign with the	
25	UK,” <i>Motherboard</i> (Feb. 10, 2016), <i>available at</i> https://motherboard.vice.com/read/new-	
26	case-suggests-the-fbi-shared-data-from-its-mass-hacking-campaign-with-the-uk	13

INTRODUCTION

The Ninth Circuit recently explained that “legitimate concerns about child pornography do not justify unfettered crime-fighting searches or an unregulated assault on citizens’ private information.” *United States v. Cotterman*, 709 F.3d 952, 966 (9th Cir. 2013) (en banc). The nature of the child pornography crime under investigation here, specifically the Playpen website, led the government to seek and a court to approve a warrant that deployed an expansive and unprecedented tool to hunt down users of the site: a piece of computer code called a Network Investigative Technique (“NIT”) that was sent to the computers of individual users and reported information about those computers back to the FBI. The government, however, did not seek to deploy this tool in the targeted, particular way required by the Fourth Amendment of the U.S. Constitution. Instead the FBI was permitted to deploy the NIT aggressively and expansively, sending it to hundreds of thousands of computers across the United States and abroad. These numerous searches and seizures were authorized by a single search warrant issued by a single magistrate judge in the Eastern District of Virginia.

It did not have to be this way; once the government had seized the Playpen site, it could have more narrowly deployed the NIT to specific users based on particularized and specific showings of probable cause. Law enforcement cannot rely on new surveillance techniques “blindly,” and “[w]ith the benefits of more efficient law enforcement mechanisms comes the burden of corresponding constitutional responsibilities.” *Arizona v. Evans*, 514 U.S. 1, 17-18 (1995) (O’Connor, J., concurring). With appropriate tailoring and sufficient specificity, a valid warrant could issue for the deployment of the NIT. But here, the government consciously chose to cast its net as broadly as possible, neglecting its constitutional responsibilities. Ultimately, that means the NIT warrant violated the Fourth Amendment’s particularity requirement and must be suppressed.

STATEMENT OF FACTS

Beginning in September 2014, FBI agents began investigating a child pornography website called “Playpen” which was accessed on the Tor computer network. The Tor network consists of a computer network and software that provide Internet users with online anonymity. Tor was initially

1 developed by the United States Naval Research Lab in the 1990s and is now run as an independent
2 non-profit organization. Tor works by obscuring how and where users access the Internet. Users
3 first download Tor software onto their computers. The software allows users to connect to the Tor
4 network, which is a network of computers—known as “nodes” or “relays”—operated by volunteers.
5 When a user connects to the Tor network, their Internet traffic does not go directly to the website
6 they are seeking. Instead, a Tor user’s Internet traffic connects to a volunteer node or relay, which
7 passes the user’s Internet traffic on to another volunteer node or relay, and then to another node or
8 relay (and perhaps many other nodes or relays) until it exits through an “exit node” and connects to
9 the site. This allows users to mask their true location when they visit a site. Specifically, the site
10 will only know the IP address of the exit node’s computer, and not the original computer that sought
11 to access the site.¹

12 Tor also provides users with other services, including an anonymous web hosting service
13 known as a “hidden service.” A Tor hidden service is a website hosted on the Tor network which
14 does not reveal its location. For example, rather than displaying a URL like www.cand.uscourts.gov,
15 the site’s location would be replaced with a Tor based web address such as dboevtdpvsuthpw.onion.
16 Tor hidden service websites end in .onion and can only be accessed through the Tor network. As a
17 result, a Tor user can connect to a Tor hidden service site without knowing the site’s location and
18 without the site knowing the visitor’s location.²

19 Playpen operated as a Tor hidden service that could only be accessed through the Tor
20 network. In order to access the site, a visitor was required to login with a username and password.
21 *See* Exhibit A, Eastern District of Virginia Search Warrant 15-SW-89 (“NIT Warrant”) at ¶ 12. Once
22 logged in, a visitor could view the content on the site, which included discussion forums, private
23 messaging services, and images of child pornography. *Id.* at ¶¶ 12-14.

24 In December 2014, a foreign law enforcement agency informed the FBI that it had a suspected
25 United States based IP address for the site. *Id.* at ¶ 28. The FBI investigated the IP address and
26

27 ¹ *See generally* <https://www.torproject.org/about/overview.html.en>.

28 ² *See generally* <https://www.torproject.org/docs/hidden-services.html.en>.

1 determined that the website was hosted on a server in Lenoir, North Carolina. *Id.* In January 2015,
2 the FBI obtained and executed a search warrant in the Western District of North Carolina, and seized
3 the server that hosted the Playpen website. *Id.* Once the government had control of the website, it
4 had a window into the activity of the site's users. *Id.* at ¶¶ 14-27. For example, it could see specific
5 posts by specific users and could tell how frequently users posted to the site. *Id.* at ¶¶ 16-19. The
6 government could view the site's users by the number of posts they made and thus determine which
7 users aggressively used the site. *See* Exh. B, Declaration of Madeline Larsen at ¶ 5. For example,
8 by the time the site was shut down on March 4, 2015, the user who had posted the most on the
9 Playpen site had made a total of 1,309 posts. *Id.* The vast majority of users of the site, however, did
10 not post onto the site at all. *Id.* at ¶ 6 (only 11,460 of the approximately 214,980 users of the site as
11 of March 4, 2015, had posted on the site).

12 Once it seized the server hosting Playpen rather than shut down the site, the FBI instead
13 placed a copy of the seized server and website, including the child pornography contained on the
14 Playpen site, onto a government controlled server in Newington, Virginia. *Id.* On February 20,
15 2015, prosecutors in the Eastern District of Virginia ("EDVA") submitted an application and
16 affidavit for a search warrant to U.S. Magistrate Judge Theresa Carroll Buchanan in Alexandria,
17 Virginia. In the affidavit, the government explained that it wanted to continue operating the Playpen
18 site from a "government-controlled computer server in Newington, Virginia, on which a copy of
19 TARGET WEBSITE currently resides." Exh. A at ¶ 30. It explained it wanted to operate the site
20 for 30 days in order to locate and identify visitors to the site. *Id.* at ¶¶ 29-30. The warrant affidavit
21 explained that in order to identify the users of Playpen, it would need to deploy an additional
22 investigative tool to work around the fact that the Tor network was obfuscating the visitor's IP
23 address. The government thus requested authorization to deploy a Network Investigative Technique
24 ("NIT") which it believed had a "reasonable likelihood" to locate administrators and users of the site.
25 *Id.* at ¶ 31; *see also* ¶¶ 32-37.

26 The NIT was simply computer software that the government inserted into the Playpen site.
27 More specifically, the NIT was "malware"—a term used to refer to malicious software that is
28

designed to disrupt or damage computer operations, as well as gather sensitive information or gain unauthorized access to a computer.³ The NIT was a form of malware known as a remote access tool, which is software that takes advantage of unpatched flaws in computer software in order to control a device and extract information from the computer without the user's knowledge or consent.⁴

According to the search warrant affidavit, the government would deploy the NIT—that is, send it to the user's computer—anytime a visitor to Playpen entered a username and password to access the site. Once a visitor to the site entered their username and password, the FBI controlled server would use the NIT to force the user's computer to collect information directly from the user's computer and then transmit that information back to the FBI. Exh. A at ¶ 36. The specific information collected by the NIT were:

- The “activating” computer's actual IP address and the date and time the NIT determined what that IP address was;
- A unique identifier generated by the NIT to distinguish the different data obtained from other “activating” computers;
- The type of operating system running on the “activating” computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86);
- Information about whether the NIT has already been delivered to the “activating” computer;
- The “activating” computer's “host name,” which is the name assigned to a device connected to a computer network used to identify the specific device;
- The “activating” computer's active operating system username; and
- The “activating” computer's Media Access Control (“MAC”) address, which is a unique identifying number associated with computers.

Id. at ¶ 34. The NIT application sought authorization to deploy the NIT to investigate “any user”

³ See Robert Moir, Defining Malware: FAQ, Microsoft TechNet (Oct. 2003), *available at* <https://technet.microsoft.com/en-us/library/dd632948.aspx>.

⁴ See Roger A. Grimes, Danger: Remote Access Trojans, Microsoft TechNet (Sept. 2002), *available at* <https://technet.microsoft.com/en-us/library/dd632947.aspx>.

1 who logged into the site with a username and password, regardless of their physical location, whether
2 or not they were using the site's chat features, or viewing child pornography. *Id.* at ¶ 32 fn. 8. But
3 the government also noted that it could deploy the NIT in other ways, explaining "in order to ensure
4 technical feasibility and avoid detection of the technique by subjects of investigation, the FBI may
5 deploy the NIT more discretely against particular users." *Id.* The warrant affidavit, however, did
6 not elaborate on what that meant, how the government would decide which users merited that
7 different treatment or what deploying the NIT "more discretely" meant. The magistrate judge signed
8 the warrant that same day and authorized the government to deploy the NIT for 30 days.

9 Equipped with the NIT warrant and a wiretap order signed by a district judge authorizing the
10 real time interception of communications on the site, the government began deploying the NIT on
11 February 20, 2015. *See* Doc. 19, Motion to Suppress NIT Warrant, Exhibit B, Eastern District of
12 Virginia Wiretap Order 15-ES-4. Although the government was authorized to deploy the NIT for 30
13 days, on March 4, 2015, it abruptly stopped deploying the NIT and took the Playpen website offline.
14 Based on information obtained by the NIT, the government identified numerous IP addresses that
15 visited the Playpen site during the time it was operated by the government.

16 One of those IP address was associated with 678 7th Street in Richmond, California, which
17 was ultimately determined to be Mr. Hammond's residence.⁵ On July 16, 2015, FBI Special Agent
18 Robert Basanez submitted an application and affidavit for a search warrant to Northern District of
19 California Magistrate Judge Maria-Elena James, seeking authorization to search Mr. Hammond's
20 apartment in Richmond. *See* Doc. 19, Motion to Suppress NIT Warrant, Exhibit C, Northern District
21 of California Search Warrant 15-70905. Judge James signed the warrant that same day. *Id.* at p. 5-7.

22 The next day, the FBI executed the search warrant in Richmond. Eight months later, a one
23 count indictment was filed on March 10, 2016, charging Mr. Hammond with possession of child
24 pornography in violation of 18 U.S.C. § 2252(a)(4)(B).

25
26
27 ⁵ After filing the motion to suppress the NIT warrant (Doc. 19), counsel for Mr. Hammond realized
28 that the motion incorrectly identified Mr. Hammond's address as 678 8th Street; it should be 678 7th
Street.

ARGUMENT

The Fourth Amendment to the U.S. Constitution states “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. CONST. AMEND. IV.

Here, the NIT both searched Mr. Hammond’s computer and seized data from it. While the government obtained a search warrant to deploy the NIT, the warrant failed to comply with one of the pillars of the Fourth Amendment: it was not particularized but instead a 21st century version of a general warrant. Thus, the NIT warrant and all of its fruits must be suppressed.

A. Each Deployment of the NIT Resulted in a Series of Invasive Searches and Seizures.

A Fourth Amendment seizure occurs when “there is some meaningful interference with an individual’s possessory interests” in property. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). A Fourth Amendment search occurs when the government either “physically occupie[s] private property for the purpose of obtaining information,” *United States v. Jones*, 132 S. Ct. 945, 949 (2012), or infringes on an individual’s “reasonable expectation of privacy.” *Katz v. United States*, 389 U.S. 347, 360-61 (1967) (Harlan, J., concurring).

The NIT warrant glosses over the significant Fourth Amendment events that occurred every time the government deployed its malware, but each NIT deployment caused three separate Fourth Amendment events to occur: (1) a seizure of Mr. Hammond’s computer; (2) a search of the private areas of that computer; and (3) a seizure of private information from the computer. That two seizures and a search occurred when the NIT was deployed is evidence of the NIT warrant’s sweeping breadth. The NIT warrant was not limited to a single search or seizure; nor was it limited to all three for a specific user. Rather, the NIT warrant ultimately authorized the FBI to repeatedly execute these searches and seizures—upwards of hundreds of thousands of times—on thousands of computers.

1 **1. The Presence of the NIT on Mr. Hammond’s Computer Was a Seizure and**
 2 **Search.**

3 When the government sent the NIT to Mr. Hammond’s computer, that malware exploited an
 4 otherwise unknown or obscure software vulnerability, turning the software against the user—and
 5 into a law enforcement investigative tool. As a result, the presence of the NIT on Mr. Hammond’s
 6 computer (even if unnoticed by Mr. Hammond), and the manipulation of the software running on his
 7 computer, constitutes a Fourth Amendment seizure and search.

8 Mr. Hammond undeniably had a possessory interest in his personal property—the computer
 9 and the software operating on those computers. The government “interfere[d]” with that possessory
 10 interest by surreptitiously placing the NIT code on his computer. Indeed, by exploiting a
 11 vulnerability in the software running on his computer, the government exercised “dominion and
 12 control” over the exploited software and thus seized Mr. Hammond’s computer. *Jacobsen*, 466 U.S.
 13 at 120-21, n.18. Similarly, even if the malware did not affect the normal operation of the software,
 14 it added a new—and unwanted—“feature:” it became a law enforcement tool for identifying Tor
 15 users. That exercise of “dominion and control,” even if limited, was a Fourth Amendment seizure.
 16 *Id.*

17 The installation and presence of the NIT onto Mr. Hammond’s computer was also a Fourth
 18 Amendment search since the government entered into Mr. Hammond’s computer in order to obtain
 19 information about him. *See Jones*, 132 S. Ct. at 949 (finding Fourth Amendment search occurred
 20 where “government physically occupied” individual’s property by attaching GPS tracker to it).

21 **2. Operating the NIT on Mr. Hammond’s Computer Was a Search.**

22 When the NIT operated on Mr. Hammond’s computer, the malware sought out certain
 23 information stored on the computer. This was a Fourth Amendment search since it intruded upon a
 24 reasonable expectation of privacy. *Katz*, 389 U.S. at 360-61.

25 There can be no real dispute that individuals have a reasonable expectation of privacy in their
 26 computers and the information stored therein. As the Supreme Court recently recognized in *Riley v.*
 27 *California*, 134 S. Ct. 2473 (2014), due to the wealth of information that electronic devices “contain
 28

1 and all they may reveal, they hold for many Americans ‘the privacies of life.’” 134 S. Ct. at 2494-95
 2 (citing *Boyd v. United States*, 116 U.S. 616, 630 (1886)). Computers “are simultaneously offices
 3 and personal diaries” and “contain the most intimate details of our lives.” *Cotterman*, 709 F.3d at
 4 964. It is no surprise that the Ninth Circuit has repeatedly recognized the need for a warrant prior to
 5 searching a computer. *See, e.g., United States v. Payton*, 573 F.3d 859, 862 (9th Cir. 2009)
 6 (“Searches of computers . . . often involve a degree of intrusiveness much greater in quantity, if not
 7 different in kind, from searches of other containers.”); *United States v. Ganoë*, 538 F.3d 1117, 1127
 8 (9th Cir. 2008) (“as a general matter an individual has an objectively reasonable expectation of
 9 privacy in his personal computer”).

10 In this case, a search occurred because the NIT operated directly on Mr. Hammond’s
 11 computer—a private area subject to a reasonable expectation of privacy. *Ganoë*, 538 F.3d at 1127.
 12 That is all that is required to give rise to a Fourth Amendment interest. *See Rakas v. Illinois*, 439
 13 U.S. 128, 143 (1978) (Fourth Amendment protection depends on “a legitimate expectation of privacy
 14 in the invaded place”).⁶ The malware operated by “searching” the computer and its memory for the
 15 following information: the computer’s IP address; the type of operating system running on the
 16 computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x
 17 86); the computer’s “Host Name”; the computer’s “active operating system username”; and
 18 “media access control (“MAC”) address.” Doc. 19, Exh. A at ¶ 34.⁷ Just as a search would have
 19 occurred if the FBI manually reviewed Mr. Hammond’s computer to locate this information, a search

21 ⁶ While some of the information obtained in the search might, in other contexts, be provided to third
 22 parties, the government did not obtain the information here from any third party. Rather, it directly
 23 searched private areas on Mr. Hammond’s computer. Thus, the so-called third party doctrine—
 24 which holds there is no Fourth Amendment expectation of privacy in information voluntarily given
 to a third party when the government seeks to *obtain it from the third party directly*—has no
 applicability here. *See Riley*, 134 S. Ct. at 2492-93 (third party doctrine did not apply when police
 directly search cell phone’s call log as opposed to records of phone calls obtained from the phone
 company); *see also* Doc. 19 at p. 14-15.

25 ⁷ Mr. Hammond is not aware of precisely how the malware operated on his computer and is awaiting
 26 additional discovery from the government on the specifics of the NIT computer code. Those
 27 specifics could affect the analysis of the invasiveness of the search—how much information the
 malware accessed and what specific areas of the computer were searched—which could be a separate
 basis for a motion to suppress. Even without those specifics, as explained above, this Court can
 conclude that a Fourth Amendment search and seizure occurred.

also occurred when the government employed technological means to interact with the computer directly and obtain the same information.

3. Copying Data From Mr. Hammond's Computer Was a Seizure.

When the NIT copied information from software running on the users' computers, the copying of that data was a second seizure. Again, a seizure occurs when the government "meaningfully interfere[s]" with an individual's possessory interest in property. *Jacobsen*, 466 U.S. at 113. Courts recognize that individuals have possessory interests in information and that copying information interferes with that interest. *See LeClair v. Hart*, 800 F.2d 692, 695, 696 n.5 (7th Cir. 1986) (recognizing it "is the information and not the paper and ink itself" that is actually seized) (quoting *Jacobsen*, 466 U.S. at 113).

"[W]hile copying the contents of a person's documents . . . does not interfere with a person's possession of those documents, it does interfere with the person's *sole* possession of the information contained in those documents." *United States v. Jefferson*, 571 F. Supp. 2d 696, 703 (E.D. Va. 2008) (emphasis added). This is because "the Fourth Amendment protects an individual's possessory interest in information itself, and not simply in the medium in which it exists." *Id.* at 702; *see also United States v. Comprehensive Drug Testing, Inc.* ("CDT"), 621 F.3d 1162, 1168-71 (9th Cir. 2010) (en banc) (per curiam) (referring to copying of data as a "seizure").

Since the government both searched and seized data from Mr. Hammond's computer, it was required to obtain a search warrant before deploying the NIT. Although the government did in fact obtain a warrant, that warrant failed to satisfy a crucial Fourth Amendment prerequisite: that it be particularized.

B. The NIT Warrant Was an Unconstitutional General Warrant.

One of the "distinct constitutional protections served by the warrant requirement" is that "those searches deemed necessary should be as limited as possible." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). The Fourth Amendment was intended to eliminate "the 'general warrant' abhorred by the colonists" which was "a general, explanatory rummaging in a person's belongings." *Id.* Thus, the Fourth Amendment requires a warrant be particular and limits searches and seizures to

1 “specific areas and things for which there is probable cause to search.” *Maryland v. Garrison*, 480
 2 U.S. 79, 84 (1987). That ensures “the search will be carefully tailored to its justifications, and will
 3 not take on the character of the wide-ranging explanatory searches the Framers intended to prohibit.”
 4 *Id.* Particularity also ensures that warrants are not issued on the basis of “vague or doubtful bases of
 5 fact.” *Go-Bart Importing Co. v. United States*, 282 U.S. 344, 357 (1931).

6 As described above, each time the malware was deployed, a series of significant searches and
 7 seizures took place. Given the significance and invasiveness of those events, particularity was
 8 critical. But the NIT warrant failed this elementary Fourth Amendment requirement.

9 **1. The Government Chose Not to Provide Additional Information in the Warrant.**

10 The obstacles to investigation posed by Tor did not justify a warrant as sweeping as the one
 11 obtained by the government here. The particularity requirement is context-dependent, and the
 12 specificity required in a warrant will vary based on the amount of information available and the scope
 13 of the search to be executed. Thus, in assessing the validity of warrants, “[o]ne of the crucial factors
 14 to be considered is the information available to the government.” *United States v. Cardwell*, 680
 15 F.2d 75, 78 (9th Cir. 1982); *see also Garrison*, 480 U.S. at 85-86 (officers who know they do not
 16 have probable cause to search a place are “plainly” obligated to exclude it from a warrant request).
 17 “Generic classification in a warrant are acceptable only when a more precise description is not
 18 possible.” *Cardwell*, 680 F.2d at 78 (quoting *United States v. Bright*, 630 F.2d 804, 812 (5th Cir.
 19 1980)).

20 Here, far more precision was possible, and thus necessary. The FBI was in possession of the
 21 server that hosted the site and had a clear window into the site’s user activity. Based on this user
 22 activity, the government could track: (1) which users were posting and the specific information they
 23 could access; (2) the frequency with which those users were doing so; and (3) the nature of the
 24 information that was posted or accessed. In other words, the government knew which *specific*
 25 Playpen users were administrators of the site and could tell which users used the site regularly and
 26 aggressively. *See* Exh. A at ¶¶ 14-27; Exh. B at ¶¶ 5-6. Law enforcement could have done more
 27 still—such as reviewing site activity for evidence of a user’s location or actual identity, issuing
 28

subpoenas for email addresses associated with user accounts, or using the site’s chat feature to engage individual users in conversations to learn more about their location or identity.⁸ The government could have thus obtained a specific NIT warrant based on specific facts and tied to specific users, authorizing NIT searches and seizures against those specific, named users and their specific computers. *See United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986) (validity of warrant depends on “whether the government was able to describe the items more particularly in light of the information available to it at the time the warrant issued”).⁹

2. The Warrant Failed to Particularly Describe What Was Being Searched and Where Those Searches Would Occur.

The NIT warrant failed to meet the requirements of particularity in myriad ways. Warrants require identification of a particular individual and the particular place to be searched. *See Maryland v. King*, 133 S. Ct. 1958, 1980 (2013) (warrant lacks particularity if “not grounded upon a sworn oath of a specific infraction by a *particular* individual, and thus not limited in scope and application”) (emphasis added). For example, an arrest warrant for a specific individual is not sufficiently particularized to give officers the “authority to enter the homes of third parties” when it “specifies only the object of a search . . . and leaves to the unfettered discretion of the police the decision as to which particular homes should be searched.” *Steagald v. United States*, 451 U.S. 204, 220 (1981). Any additional person or place to be searched requires a specific description in the warrant and an

⁸ In the wiretap affidavit, the government claimed traditional investigative techniques were unlikely to succeed. Doc. 19, Exh. B at ¶¶ 63-76. But they never explained any of those details *in the NIT warrant affidavit* to the magistrate judge who authorized the expansive deployment of the NIT. Any attempt by the government to incorporate other documents into the NIT warrant affidavit had to be explicit in the NIT warrant itself. *See United States v. Hill*, 459 F.3d 966, 975-76 (9th Cir. 2006) (“We do not approve of issuing warrants authorizing blanket removal of all computer storage media for later examination when there is no affidavit giving a reasonable explanation...as to why a wholesale seizure is necessary.”); *see also Groh v. Ramirez*, 540 U.S. 551, 558 (2004) (“We do not say that the Fourth Amendment prohibits a warrant from cross-referencing other documents...But in this case the warrant did not incorporate other documents by reference, nor did either the affidavit or the application (which had been placed under seal) accompany the warrant. Hence, we need not further explore the matter of incorporation.”).

⁹ Although the government eventually did obtain a warrant specific to Mr. Hammond, that was only *after* it deployed the NIT expansively and *after* it had searched his computer and seized data from it. Regardless of what steps it could have taken *before* it deployed the NIT here, it was ultimately the un-particularized and unconstitutional NIT warrant that resulted in the search of Mr. Hammond’s computer.

1 individualized showing of probable cause. *See Greenstreet v. Cnty. of San Bernardino*, 41 F.3d
 2 1306, 1309 (9th Cir. 1994); *see also Walter v. United States*, 447 U.S. 649, 656-57 (1980) (“a warrant
 3 to search for a stolen refrigerator would not authorize the opening of desk drawers.”).

4 The NIT warrant here did not name any specific person. Nor did it identify any specific user
 5 of the targeted website. It did not attempt to describe any series or group of particular users. Nor did
 6 it identify any particular computer to be searched, or even a particular type of device. Exh. A at
 7 Attachment A. Instead, the NIT warrant broadly encompassed the computer of “any user or
 8 administrator” of the website, regardless of whether they were a user of the site, an academic
 9 researcher,¹⁰ an undercover officer from another law enforcement agency,¹¹ or a person who only
 10 logged on to legally read fictional pornographic stories.¹² Significantly, there were approximately
 11 “158,094 total members” to the site at the time the government requested the NIT warrant. Exh. A
 12 at ¶ 11. The NIT warrant, on its face, thus authorized the searches and seizures described earlier for
 13 as many as 158,094 individuals’ computers.

14 Compounding matters, the NIT warrant failed to provide any specificity about *where* the
 15 searches would be carried out—the location of the “activating computers.”¹³ Instead, the NIT
 16 warrant authorized the search of “any” activating computer, no matter *where* that computer might be
 17 located. Exh. A at Attachment A. Because an activating computer could conceivably be located
 18 anywhere in the world, the Warrant authorized FBI searches and seizures in all 50 U.S. states, every
 19

20 ¹⁰ See Andy Greenberg, “Over 80 Percent of Dark-Web Visits Relate to Pedophilia, Study Finds,”
 21 *Wired*, Dec. 30, 2014, available at <https://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/> (reporting on University of Portsmouth study where researchers ran
 22 Tor relays, visited the Tor hidden service sites visited by Tor users that used these relays and
 classified each site by its content).

23 ¹¹ See e.g., *United States v. Gourde*, 440 F.3d 1065, 1067 (9th Cir. 2006) (undercover agent logged
 onto child pornography site).

24 ¹² See Exh. A at ¶ 14 (section of Playpen website devoted to fictional stories); *see also Ashcroft v.*
 25 *Free Speech Coalition*, 535 U.S. 234, 250 (2002) (First Amendment prohibits criminalization of
 pornographic speech “that records no crime and creates no victims by its production.”).

26 ¹³ The NIT warrant claimed the location of the property to be searched was the government server
 27 hosting the Playpen website in the Eastern District of Virginia. Doc. 19, Exh. A, Attachment A
 (“place to be searched” is “computer server” operating the website). But as explained earlier, and in
 28 Mr. Hammond’s previously filed motion to suppress, that is incorrect: the searches occurred on the
 user’s specific computers, wherever they were located. *See* Doc. 19 at p. 8-11.

U.S. territory, and every country around the world.¹⁴ The fact that the searches could take place in a foreign country raises significant red flags because U.S. magistrate judges have no legal authority to issue a warrant to seize or search data located abroad. *See* Fed. R. Crim. P. 41(b) (limiting magistrate judge’s authority to authorize a search to particular U.S. districts, territories, possessions or diplomatic or consular properties located abroad); *see also In re Warrant to Search A Certain Email Account*, ___ F.3d ___, 2016 WL 377056, *8 (2d Cir. Jul. 14, 2016); *In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 157, 169 (2d Cir. 2008). Thus, the breadth of the NIT warrant was virtually unbounded.

“Search warrants . . . are fundamentally offensive to the underlying principles of the Fourth Amendment when they are so bountiful and expansive in their language that they constitute a virtual, all-encompassing dragnet.” *United States v. Bridges*, 344 F.3d 1010, 1016 (9th Cir. 2003). Such is the case here: the government obtained a single warrant, authorizing the search of upwards of 159,000 users located around the world. That is far closer to a “virtual, all-encompassing dragnet” than a specific, particularized warrant required by the Fourth Amendment. *Bridges*, 344 F.3d at 1016.

3. The Warrant Vested Too Much Discretion in the Executing Officers.

The Fourth Amendment’s particularity requirement makes general searches “impossible” by ensuring that, when it comes to what can be searched or seized, “nothing is left to the discretion of the officer executing the warrant.” *Marron v. United States*, 275 U.S. 192, 196 (1927); *see also Stanford v. Texas*, 379 U.S. 476, 481 (1965) (particularity helps eliminate the threat of “officers acting under the unbridled authority of a general warrant”).

As a result of its breadth—authorizing the search of “any” activating computer regardless of where it was located—the NIT warrant gave executing officers total discretion to decide which users

¹⁴ Indeed, it appears that the government did conduct overseas searches based on the NIT warrant. *See* Joseph Cox, “FBI’s Mass Hack Hit 50 Computers in Austria,” *Motherboard* (Jul. 28, 2016), available at <https://motherboard.vice.com/read/fbis-mass-hack-playpen-operation-pacifier-hit-50-computers-in-austria>; Joseph Cox, “New Case Suggests the FBI Shared Data from Its Mass Hacking Campaign with the UK,” *Motherboard* (Feb. 10, 2016), available at <https://motherboard.vice.com/read/new-case-suggests-the-fbi-shared-data-from-its-mass-hacking-campaign-with-the-uk>.

1 to target and the manner in which to accomplish the searches and seizures. It thus left to the FBI to
2 decide how the NIT would be deployed, how the NIT operated, what portions of the activating
3 computers the NIT would search, and which of the hundreds of thousands of users of the site the NIT
4 would be deployed against.

5 In fact, the warrant application explicitly sought that discretion. As the government
6 explained, “in order to ensure technical feasibility and avoid detection of the technique by subjects
7 of investigation, the FBI may deploy the NIT more discretely against particular users.” Exh. A at ¶
8 32 n. 8. Thus, the government deployed different types of malware (or the same malware, in different
9 ways) against different users without providing any explanation of how and when these distinctions
10 would be made. Thus, the NIT warrant permitted the government to conduct its searches and seizures
11 in different ways against different users—all at the FBI’s discretion.

12 Particularly absent from the warrant was some meaningful limitation on the operation of the
13 NIT. Given that the malware effectuated a search of a user’s private computer, this type of tailoring
14 was critical. *See CDT*, 621 F.3d at 1168-71. Despite its facial appeal, the FBI’s request to act at its
15 own discretion is further evidence of a constitutional violation. *See Groh*, 540 U.S. at 560-61 (“Even
16 though petitioner acted with restraint in conducting the search, the inescapable fact is that this
17 restraint was imposed by the agents themselves, not by a judicial officer.”) (citing *Katz*, 389 U.S. at
18 356). Warrants, and the particularity requirement specifically, are designed so that the searches
19 authorized are “as limited as possible.” *Coolidge*, 403 U.S. at 467. That was not the case here: the
20 government cast its net as widely as possible and, at its own election, decided who it would target
21 and in what manner. But leaving the operation of a “dragnet” to the “discretion of the State” is
22 “fundamentally offensive to the underlying principles of the Fourth Amendment.” *Bridges*, 344 F.3d
23 at 1016.

24 Thus, the NIT warrant violated the Fourth Amendment and the warrant and all other evidence
25 “obtained as a product of illegal searches and seizures”—including the identification of Mr.
26 Hammond’s IP address—must be suppressed. *United States v. Crawford*, 372 F.3d 1048, 1054 (9th
27 Cir. 2004) (en banc) (citing *Wong Sun v. United States*, 371 U.S. 471, 484-88 (1963)). That extends
28

1 to evidence seized from the Richmond search warrant, including but not limited to any evidence
2 seized from Mr. Hammond's computer, which was a "fruit" of the original illegal NIT search
3 warrant. *See United States v. Duran-Orozco*, 192 F.3d 1277, 1281 (9th Cir. 1999).

4 **CONCLUSION**

5 The government could have more specifically tailored the NIT search warrant in order to
6 narrow its scope and avoid the unprecedented expansive search that occurred here. Because the NIT
7 warrant was not particularized, it violated the Fourth Amendment and the warrant and all of its fruits
8 must be suppressed.

9
10 DATED: August 4, 2016

STEVEN G. KALAR
Federal Public Defender

11
12 /S/
HANNI M. FAKHOURY
Assistant Federal Public Defender
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28